Claims

1. A crypto algorithm unit comprising:

a first crypto hash execution module; and

a second crypto hash execution module, wherein the first crypto execution and the second crypto execution module share a plurality of components to form a combination crypto algorithm unit.

2. The crypto algorithm unit of claim 1, wherein the combination crypto algorithm unit includes a plurality of muxes.

3. The crypto algorithm unit of claim 2, wherein the plurality of muxes provides a crypto hash algorithm selection control.

4. The crypto algorithm unit of claim 3, wherein the crypto hash algorithm selection control allows the selection of a first subset of the plurality of components, wherein the selected first subset of the plurality of components can execute a first crypto algorithm.

5. The crypto algorithm unit of claim 1, wherein the combination crypto algorithm unit is capable of executing at least two different crypto algorithms.

6. The crypto algorithm unit of claim 1, wherein the first crypto hash execution module is capable of executing at least one of a group of crypto hash algorithms consisting of an MD5 hash algorithm, a SHA-1 hash algorithm, a SHA256 hash algorithm, a SHA384 hash algorithm, and a SHA512 hash algorithm.

7. The crypto algorithm unit of claim 6, wherein the second crypto hash execution module is capable of executing at least one of a group of crypto hash algorithms consisting of an MD5 hash algorithm, a SHA-1 hash algorithm, a SHA256 hash

algorithm, a SHA384 hash algorithm, and a SHA512 hash algorithm that is different from the crypto hash algorithm that the first crypto hash execution module is capable of executing.

8. The crypto algorithm unit of claim 1, wherein the combination crypto algorithm unit is on a single integrated circuit die.

9. The crypto algorithm unit of claim 1, wherein the combination crypto algorithm unit and a microprocessor are on a single integrated circuit die.

10. The crypto algorithm unit of claim 1, wherein the combination crypto algorithm unit includes one or more full adders.

11. The crypto algorithm unit of claim 1, wherein the combination crypto algorithm unit includes one or more carry look-ahead adders.

12. The crypto algorithm unit of claim 1, wherein the combination crypto algorithm unit includes one or more compressors.

13. The crypto algorithm unit of claim 12, wherein the one or more compressors includes a group of a 4 to 2 compressor.

14. An integrated circuit comprising:

a microprocessor core; and

a combination crypto algorithm unit, the combination crypto algorithm unit being coupled to the microprocessor core.

15. The integrated circuit of claim 14, wherein the combination crypto algorithm unit is capable of executing at least two different crypto hash algorithms.

16. The integrated circuit of claim 14, wherein the combination crypto algorithm unit includes a first crypto hash execution module and a second crypto hash execution module.

17. The integrated circuit of claim 16, wherein the first crypto hash execution module is capable of executing at least one of a group of crypto hash algorithms consisting of an MD5 hash algorithm, a SHA-1 hash algorithm, a SHA256 hash algorithm, a SHA384 hash algorithm, and a SHA512 hash algorithm.

18. The integrated circuit of claim 17, wherein the second crypto hash execution module is capable of executing at least one of a group of crypto hash algorithms consisting of an MD5 hash algorithm, a SHA-1 hash algorithm, a SHA256 hash algorithm, a SHA384 hash algorithm, and a SHA512 hash algorithm that is different from the crypto hash algorithm that the first crypto hash execution module is capable of executing.

19. A method of executing a crypto instruction comprising:

receiving a first crypto hash instruction in a combination crypto algorithm unit;

determining a corresponding first crypto hash algorithm for the first crypto instruction;

selecting a first plurality of components in the combination crypto algorithm unit; and

executing the first crypto hash instruction through the selected first plurality of components.

20. The method of claim 19, further comprising:

receiving a second crypto hash instruction in the combination crypto algorithm unit;

determining a corresponding second crypto hash algorithm for the second crypto hash instruction;

selecting a second plurality of components in the combination crypto algorithm unit; and

executing the second crypto hash instruction through the selected second plurality of components, the selected second plurality of components and the selected first plurality of components sharing a third plurality of components.